Traffic Analysis of Mark Angel Store

Date: August 1, 2025

Tool Used: Wireshark

Focus: TCP Handshake Validation | TLS Session Initiation | Host Attribution

Objective

To conduct a structured forensic analysis of encrypted web traffic between a client machine and the Markangel Stores web server, focusing on handshake validation, TLS session initiation, and IP attribution.

Scope of Work:

This analysis reviewed a PCAP capture involving access to the Markangel Stores website. The primary objective was to dissect the early stages of the communication, emphasising the TCP three-way handshake and the start of encrypted (TLS) traffic. The session was assessed to determine the legitimacy of the connection, the identities of the client and server, and the nature of encrypted communication.

Key Findings:

What is the IP address of the webserver hosting Markangel Stores? 63.250.43.1

What is the IP Address of the machine used to access the markangel website? 10.10.10.162

What is the timestamp of the TCP synchronization request made to markangel stores (YYYY-MM-DD HH:MM:SS)? 2024-10-26 11:15:17.486013

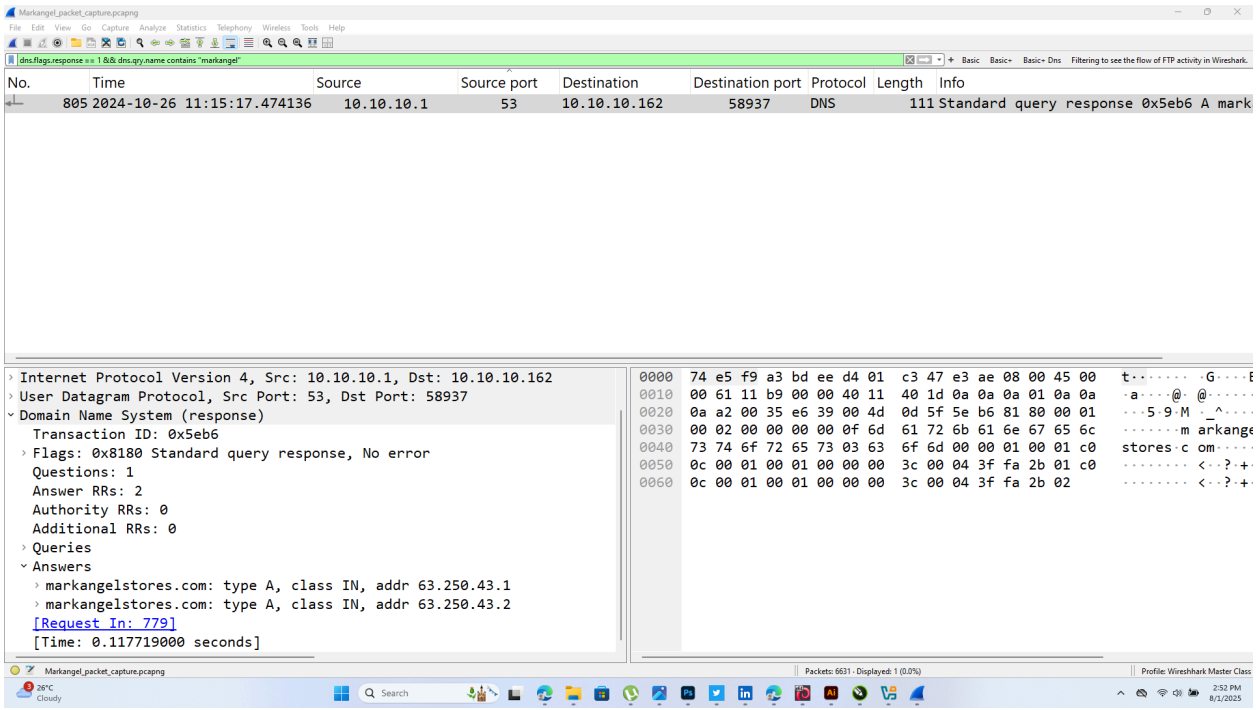
What is the source IP of the first SYN-ACK packet? 104.86.110.241

What is the packet length of the first browser acknowledgement of the SYN ACK response from the markangel webserver? 54bytes

What is the packet length and info of the first communication in the TLS handshake? 430 byte

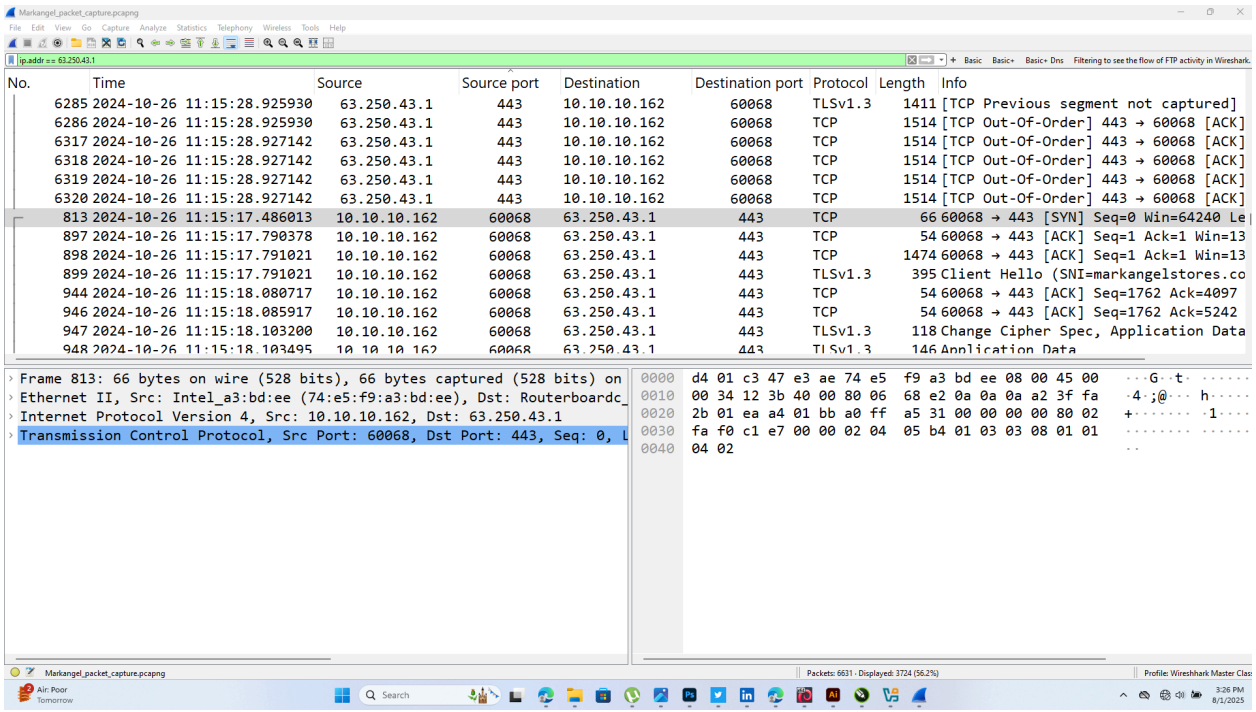
IP Address of the Web Server Hosting Markangel Stores: 63.250.43.1

This is the destination IP address contacted by the client machine when attempting to access the Markangel Stores web service. It represents the web server hosting the site and is critical for identifying the target server of interest during traffic inspection or incident investigation



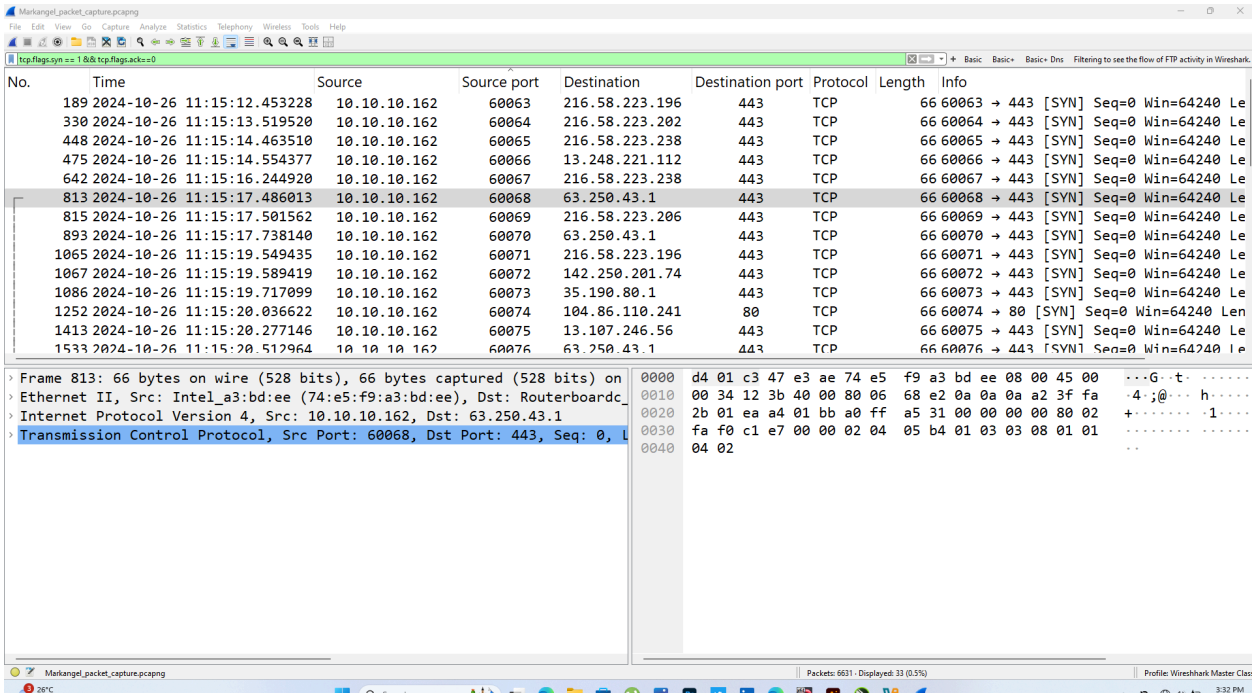
IP Address of the Machine Used to Access the Markangel Website: 10.10.10.162

This is the source IP address observed in the packet capture, which is likely to belong to a device within a private internal network. It identifies the device initiating the request to the Markangel web server. This helps trace user activity or infected endpoints in an investigation



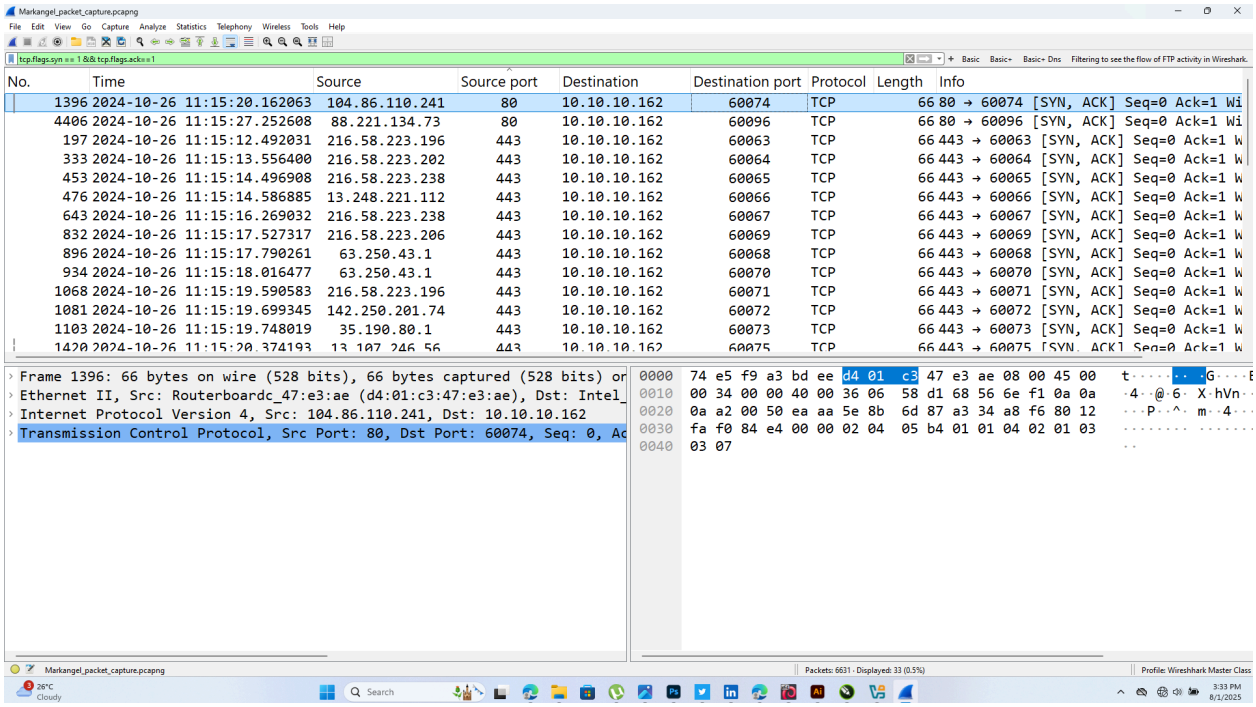
Timestamp of the TCP Synchronization (SYN) Request: 2024-10-26 11:15:17.486013

This timestamp marks the exact moment the client initiated a TCP three-way handshake to the Markangel web server. It is useful for creating a timeline of activity, identifying when a session began, and correlating with other system or application logs for deeper analysis.



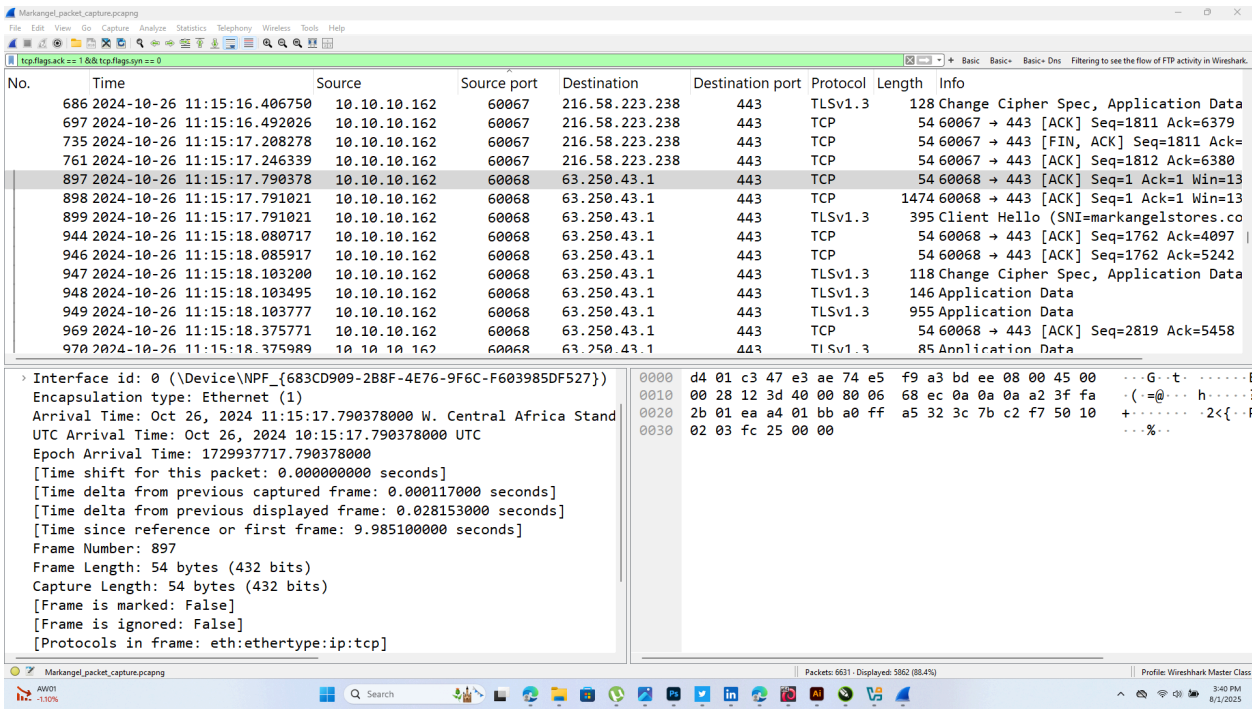
Source IP of the First SYN-ACK Packet: 104.86.110.241

This IP is the actual source of the SYN-ACK response, indicating the server endpoint that responded to the client. It may reflect a CDN (Content Delivery Network) or a load-balanced proxy in front of the actual Markangel server. This highlights the infrastructure setup and redirection path used in web hosting.



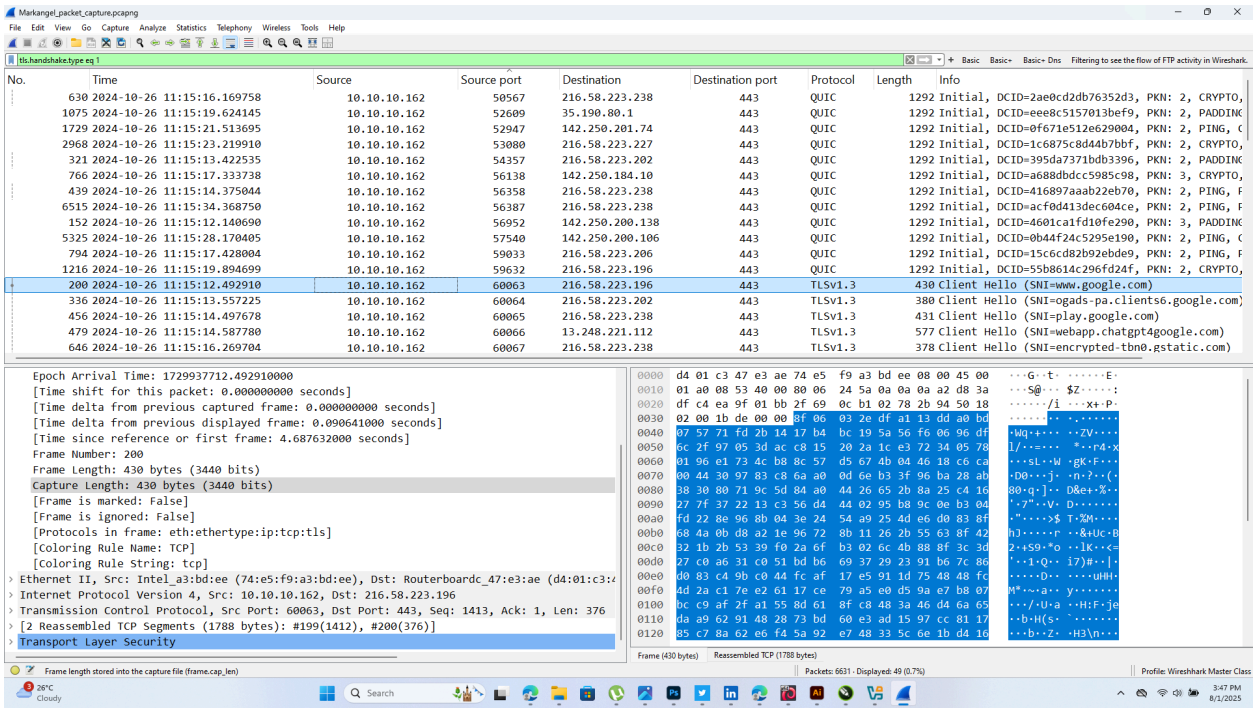
Packet Length of First Browser Acknowledgement (ACK): 54 bytes

The 54-byte ACK packet from the client confirms receipt of the SYN-ACK, completing the TCP handshake. Although small, this packet is crucial for session establishment and offers valuable insights into the normal flow of communication initiation.



Packet Length and Info of First TLS Handshake Communication: 430 bytes

The initial packet in the TLS handshake from the client is 430 bytes and typically contains the Client Hello message. This begins the encrypted session setup and may include the TLS version, supported cypher suites, and extensions. It signifies the transition from plain TCP to encrypted HTTPS traffic.



Conclusion

The network traffic analysis reveals a standard, well-structured communication session between a client device (IP: 10.10.10.162) and the Markangel Stores web server (63.250.43.1). The TCP three-way handshake was completed, with the first SYN initiated at 2024-10-26 11:15:17.486013 and a SYN-ACK response from 104.86.110.241, indicating possible use of a CDN or load balancer.

The handshake was followed by a proper TLS handshake, with the initial Client Hello packet being 430 bytes in size, signalling the start of

encrypted communication. All observed packet lengths and timestamps align with normal browser-based web access behaviour, with no evidence of malicious payloads, unusual port usage, or packet anomalies.

This analysis provides a clear baseline for typical secure client-server interaction over HTTPS and can be referenced for future anomaly detection, behavioural baselining, or threat hunting activities.